

معلومات الكاتب

الكاتب : ezat

المنتدى : شبكة ومنتديات الرقة

البريد : raqqanetworks@gmail.com

البلد : سوريا – الرقة

محرر نهج المجموعة المحلي "اعدادات النظام المتقدمة"

local Group Policy Editor

شرح بالصور لطريقة

التخلص من اضرار الفيروسات في النظام واصلاحها

بســـم الله الـرحـمن الـرحــيم

مقدمة:

محرر نهج المجموعة المحلي للكمبيوتر هي الاعدادات المقدمة للنظام مثل : السماح للمستخدم بالوصول الى محرر الرجيستري أو السماح بالوصول الى أدارة المهام......الخ

والتي تقوم الفيروسات بإيقافها بأمر واحد وبسرعة وبطريقة مختصرة .

الآن كيف يمكن تشغيل الرجيستري او ادارة المهام او موجه الاوامر... اذا تم ايقافه من قبل فيروس !

نبدأ على بركة الله

كيف نصل الى محرر نهج المجموعة المحلي ؟

على نظام

Win xp

ندخل

أبدا – تشغيل

ونكتب الامر

Gpedit.msc

موافق

****

أما في نظام win7

ابدا – كافة البرامج – البرامج الملحقة – تشغيل

ونضع نفس الامر

Gpedit.msc

موافق

** بإمكانك نسخ الامر ولصقه **

كما في الصورة :



شبكة ومنتديات الرقة

ملاحظة : لتسـهيل حفظنا الامر gpedit.msc نقوم بتحليله ومعرفة معناه

هي اختصار لـ **Group Policy Editor** أي محرر نهج المجموعة

حيث حرف g هو اختصار لـ group اي مجموعة

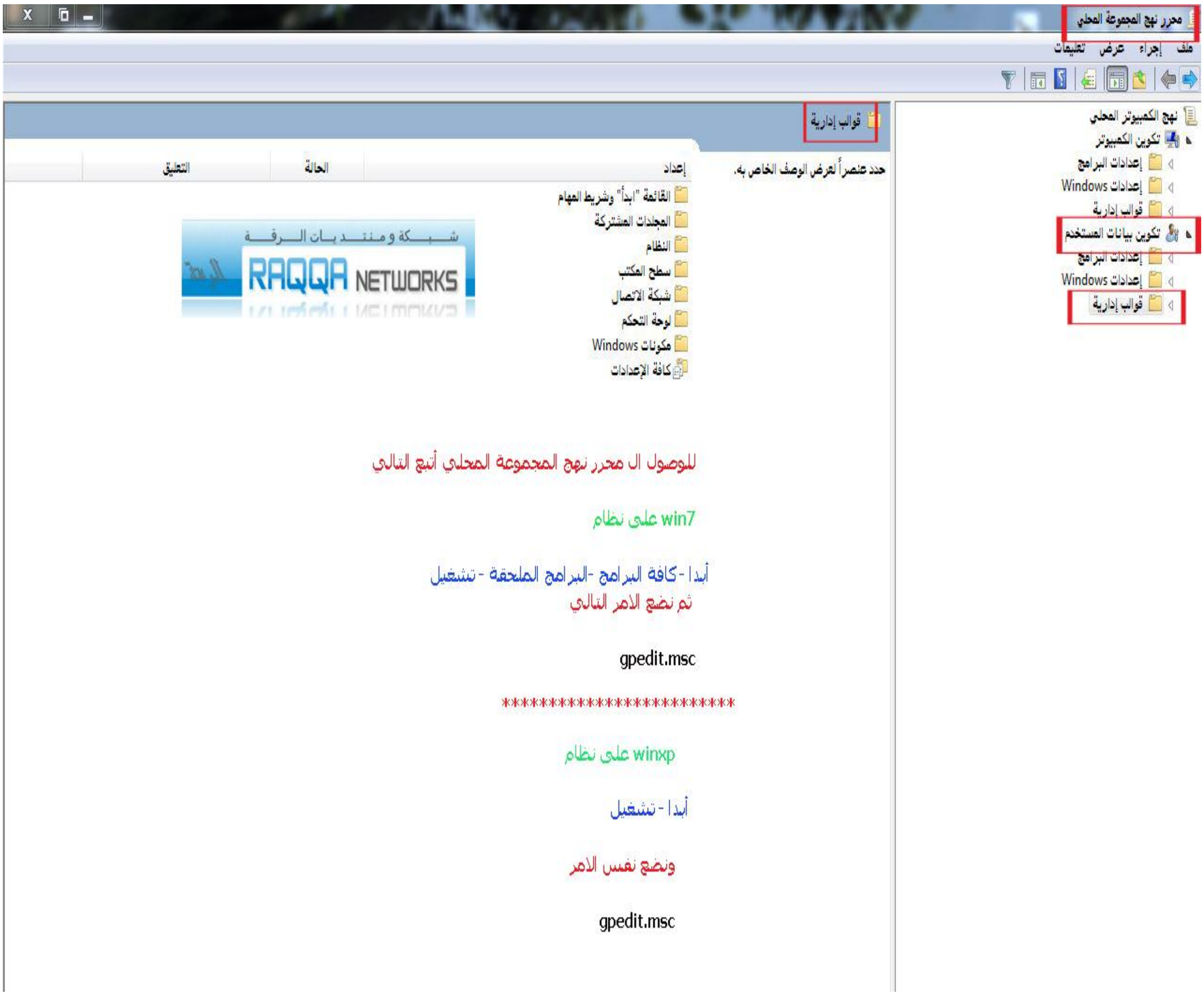
وحرف p هو اختصار لـ policy أي نهج

و Edit هو اختصار لـ **Editor** **أي** **محرر**

أما msc هي لاحقة البرنامج مثل exe و swf الخ...... و لا تنسى وضع نقطة (.)

ملاحظة : البرنامج في كل الانظمة مثبت تلقائيا .

الآن نتعرف على واجهة محرر نهج المجموعة المحلي



صورة توضح محرر نهج المجموعة المحلي

طبعا الذي يهمنا القسم :

* تكوين بيانات المستخدم *

الان بعد كل هذا الشرح المطوّل لطريقة الوصول الى محرر نهج المجموعة نبدأ العمل !

---

١ - حل مشكلة تم تعطيل الرجيستري من قبل المسؤول

الرجيستري مهم جدا في تسجيل البرامج أو الالعاب... الخ في النظام .

يقوم الفيروس عند دخوله الى جهازك بتعطيل الرجيستري وهو لا يقوم بحذف برنامج الرجيستري كما يعتقد البعض بل يقوم بإيقافه من محرر نهج المجموعة

كالتالي:

منع الوصول الى ادوات تحرير الرجيستري

فيختار الفيروس : ممكن

ونحن سنقوم بالتعديل الى :معطل

أو : غير مكون

لكي نستطيع تشغيل الرجيستري.

حل المشكلة :

نقوم بالدخول الى محرر المجموعة المحلي (شرحت طريقة الوصول الى المحرر في الاعلى)

بالأمر gpedit.msc

وندخل كالتالي :

١- محرر نهج الكمبيوتر المحلي ٢– تكوين بيانات المستخدم ٣– قوالب ادارية ٤ – النظام

٥- منع الوصول الى ادوات محرر الرجيستري

ونضغط عليه نقرتين :ونختار

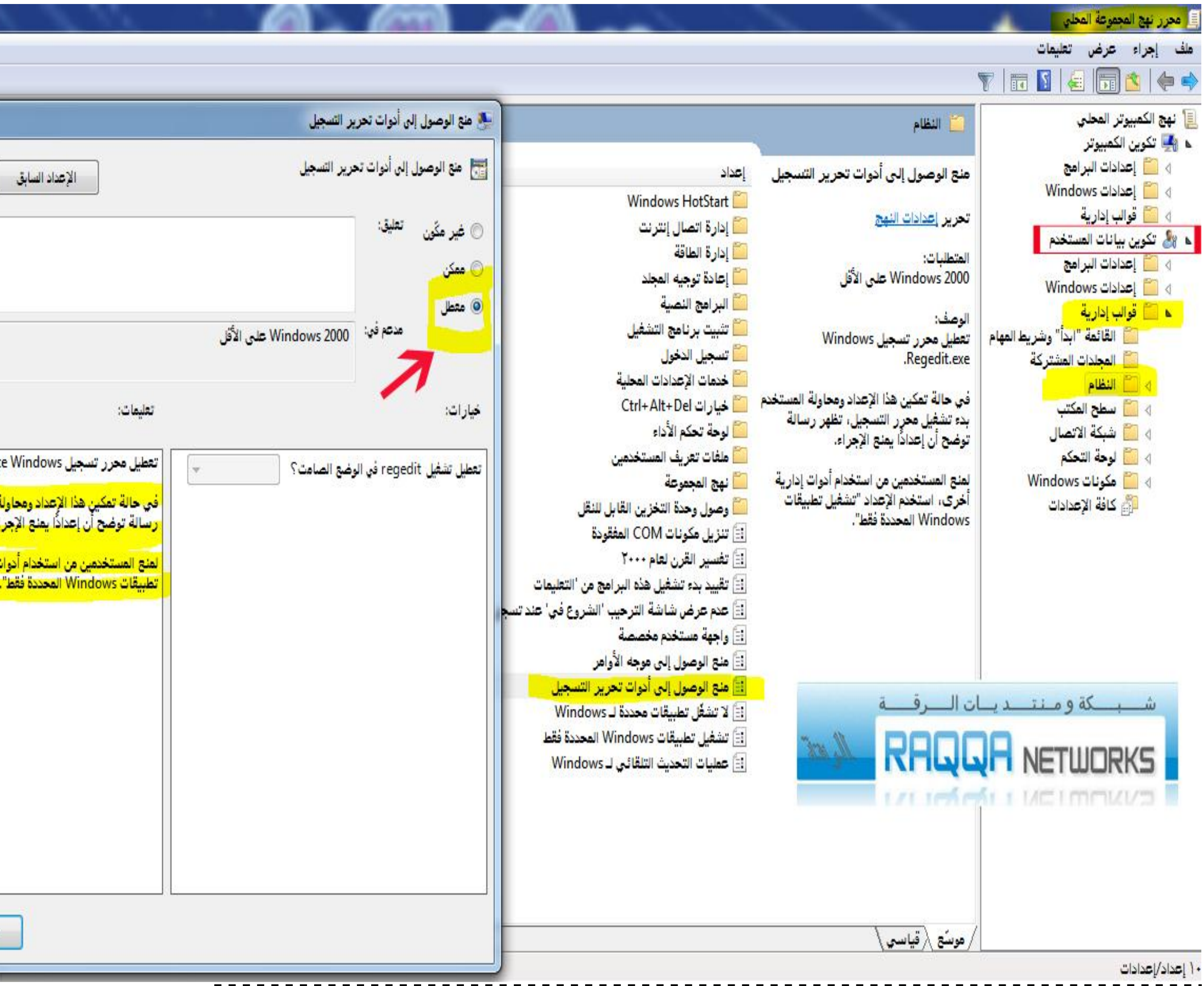
معطل   أو غير مكون   أي تلقائي

ثم

موافق

ويتم تشغيل الرجيستري

شرح بالصور لطريقة تشغيل الرجيستري :



صورة تبيّن طريقة تشغيل الرجيستري

٢- حل مشكلة تم ايقاف ادارة المهام من قبل المسؤول أو ctrl+alt+delete

Taskmanegar

ادارة المهام

مهم جدا في مراقب العمليات التي تعمل في الخلفية وأنهاء البرامج التي لا تستجيب ......الخ

"مثل الرجيستري"

يقوم الفيروس بمنع المستخدم من الوصول الى ادارة المهام

(لا تنسى عن طريق محرر المجموعة المحلي)

الامر

gpedit.msc

****أنسخ الامر واللصقه****

كالتالي:

خيارات ctrl+alt+delete

ثم

ازالة ادارة المهام

الفيروس يعمل: ممكن

ونحن نعمل :معطل أو غير مكون

حل المشكلة:

ندخل :

محرر نهج المجموعة المحلي

+

تكوين بيانات المستخدم + قوالب ادارية + النظام + خيارات ctrl+alt+delete نـنقر عليها مرتين

فتظهر

ازالة ادارة المهام

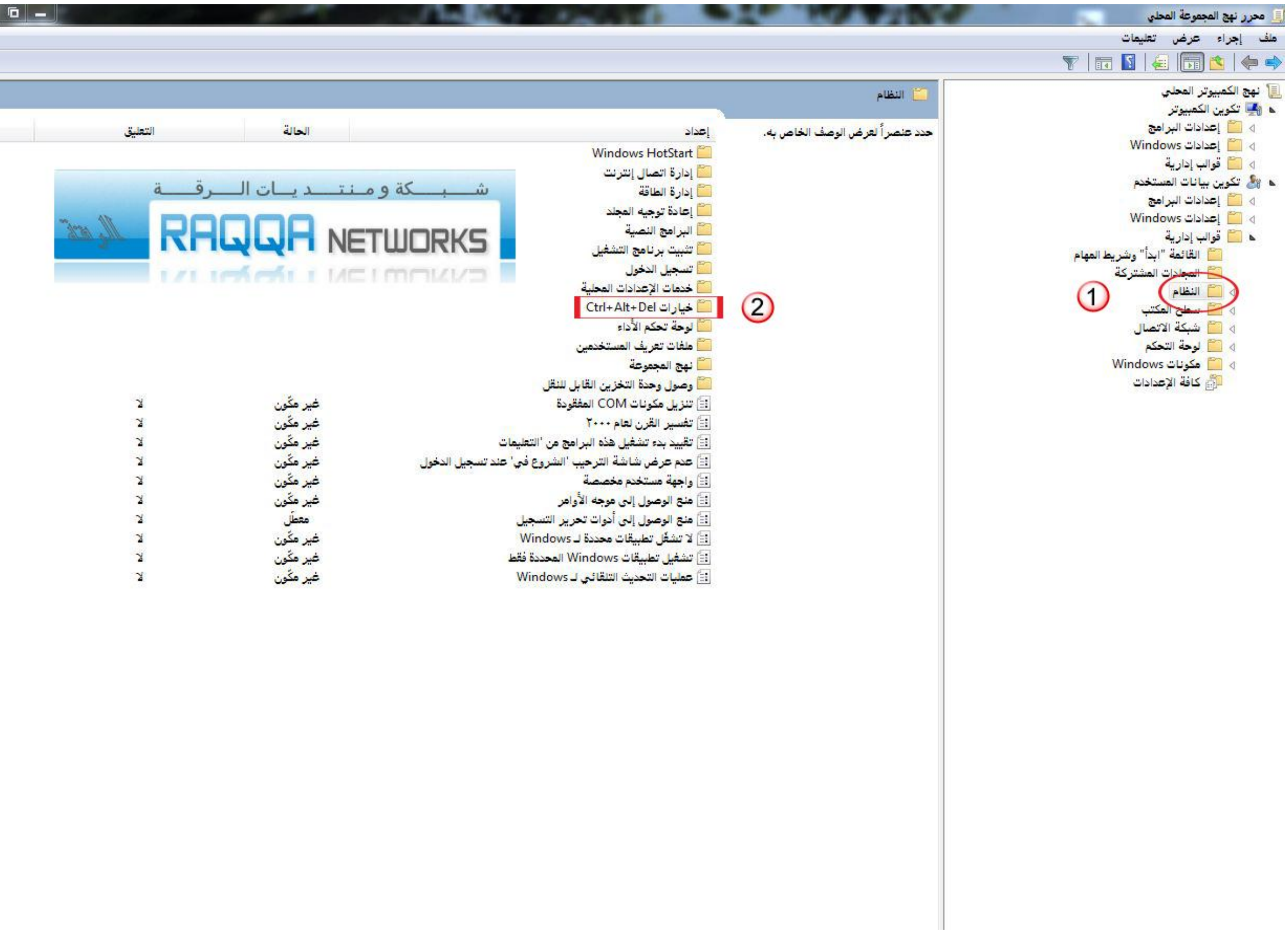
وننقر مرتين

وتظهر لنا الخيارات

فنختار

معطل أو غير مكون

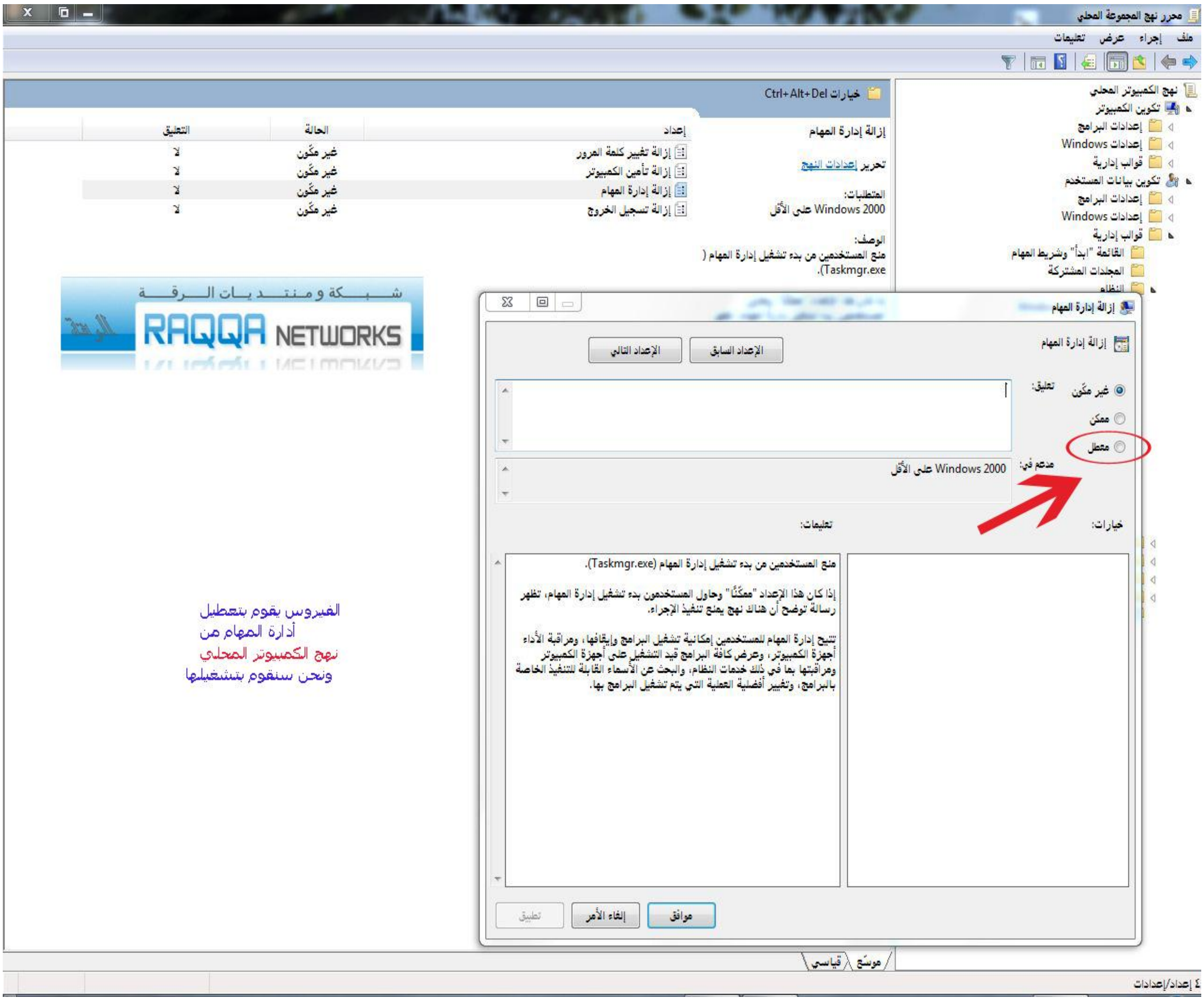
شرح بالصور لطريقة تشغيل ادارة المهام :



ننقر مرتين على خيارات ctrl+alt+del

فتظهر لنا

كالصورة :



ازالة ادارة المهام نختار معطل

٣ – حل مشكلة أيقاف موجه الاوامر :

موجه الاوامر :

Run

اداة مهمة للذين يتعاملون مع بيئة DOS الدوس

المشكلة كالتالي :

The command prompt has been disabled by your administrator.

موجه الاوامر تم تعطيله من قبل المدير "المسؤول".

لاحظ الصورة :



عمل الفيروس:

منع المستخدم من الوصول الى موجه الاوامر

(طبعا عن طريق محرر المجموعة المحلي)

حل المشكلة :

ندخل الى محرر المجموعة المحلي (ذكرنا طريقة الوصول اليها)

عن طريق الامر : gpedit.msc

+

تكوين بيانات المستخدم + قوالب ادارية + النظام + منع الوصول الى موجه الاوامر

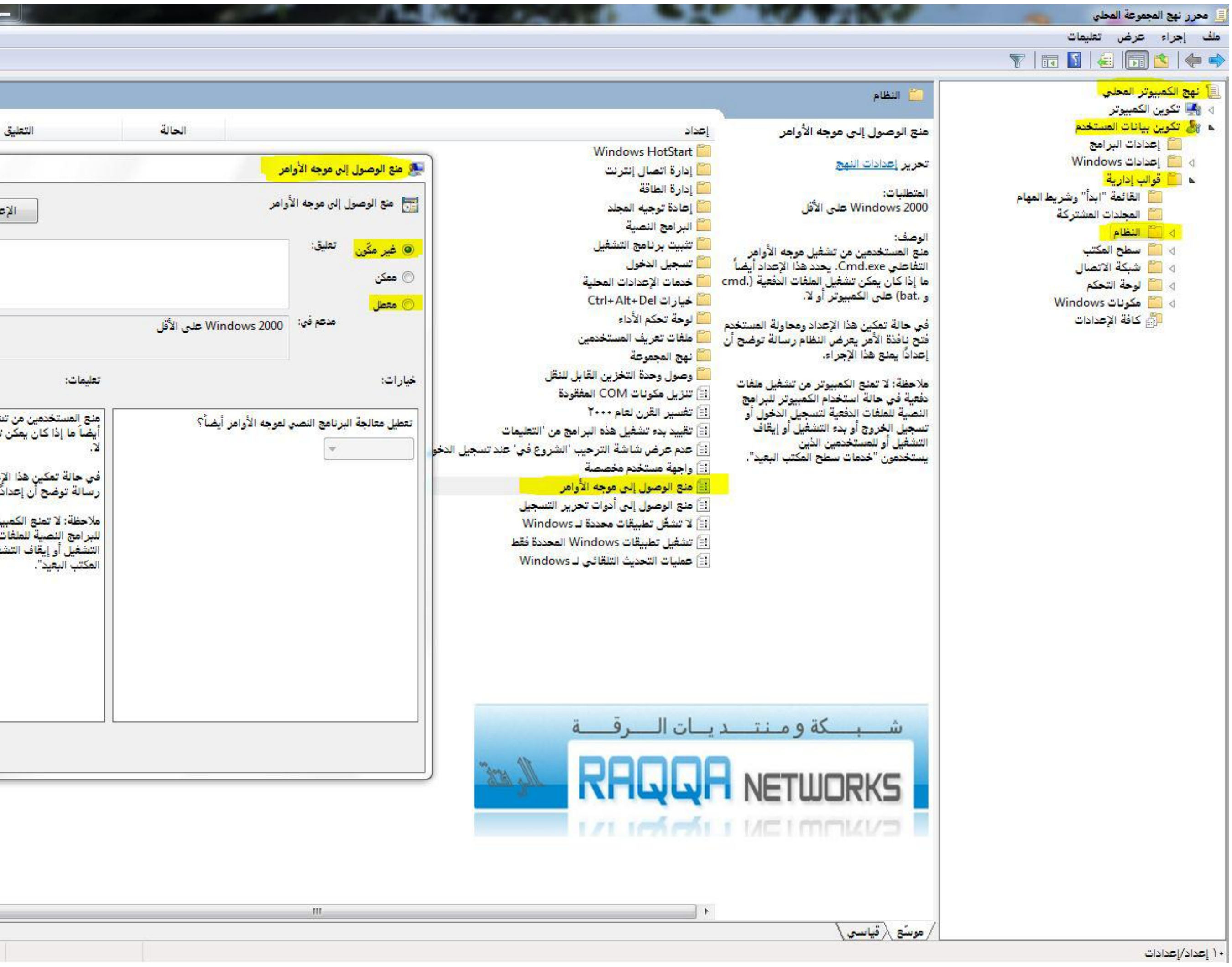
ونختار:

معطل أو غير مكون

موافق

شرح بالصور :

....



صورة توضح طريقة تشغيل / ايقاف محرر الاوامر

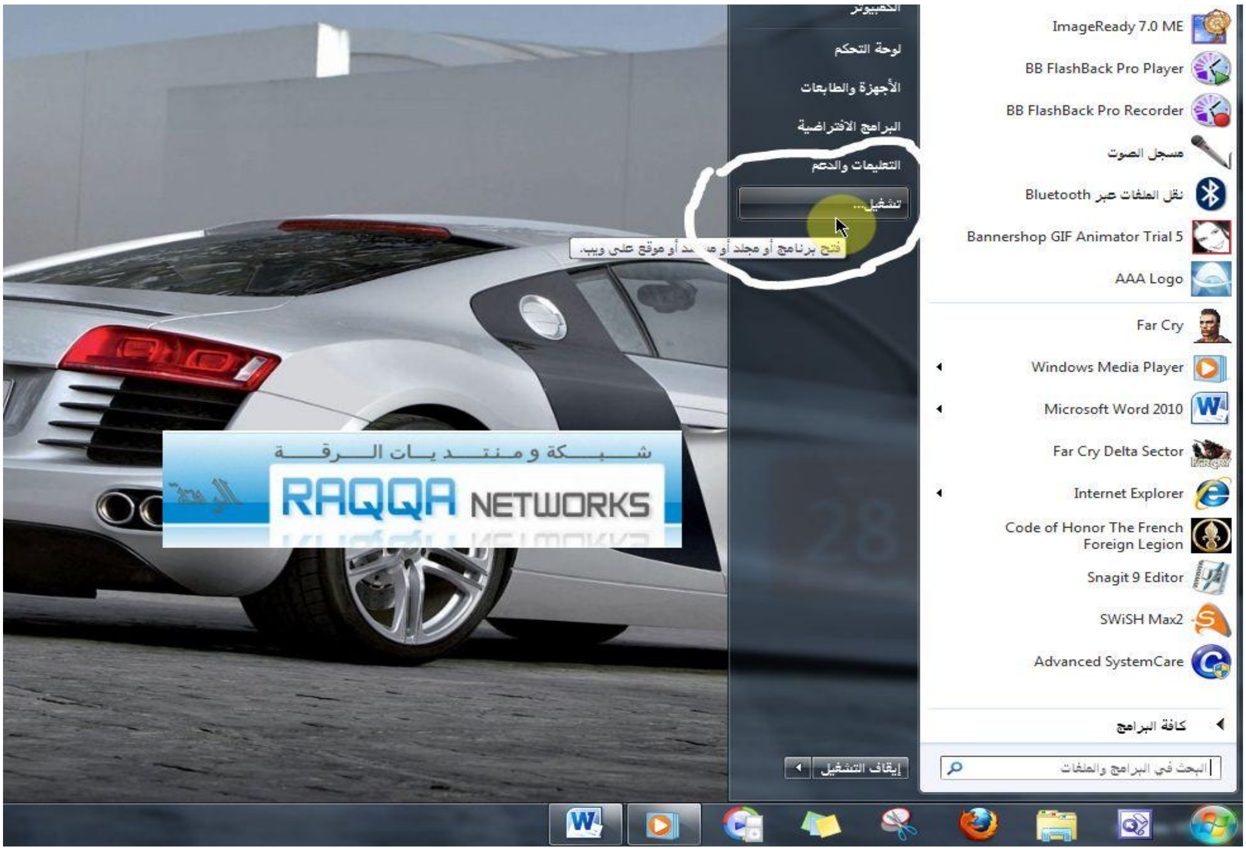
٤ – طريقة أضافة الامر تشغيل الى القائمة أبدأ على نظام win7

مربع الحوار تشغيل لا يوجد في القائمة أبدا مباشرة في نظام win 7 يكون موجود في البرامج الملحقة

سنشرح طريقة أضافته

لاحظ الصورة :

:



صورة توضح مكان الامر تشغيل في القائمة أبدا مباشرة على نظام win7

طريقة الاضافة :

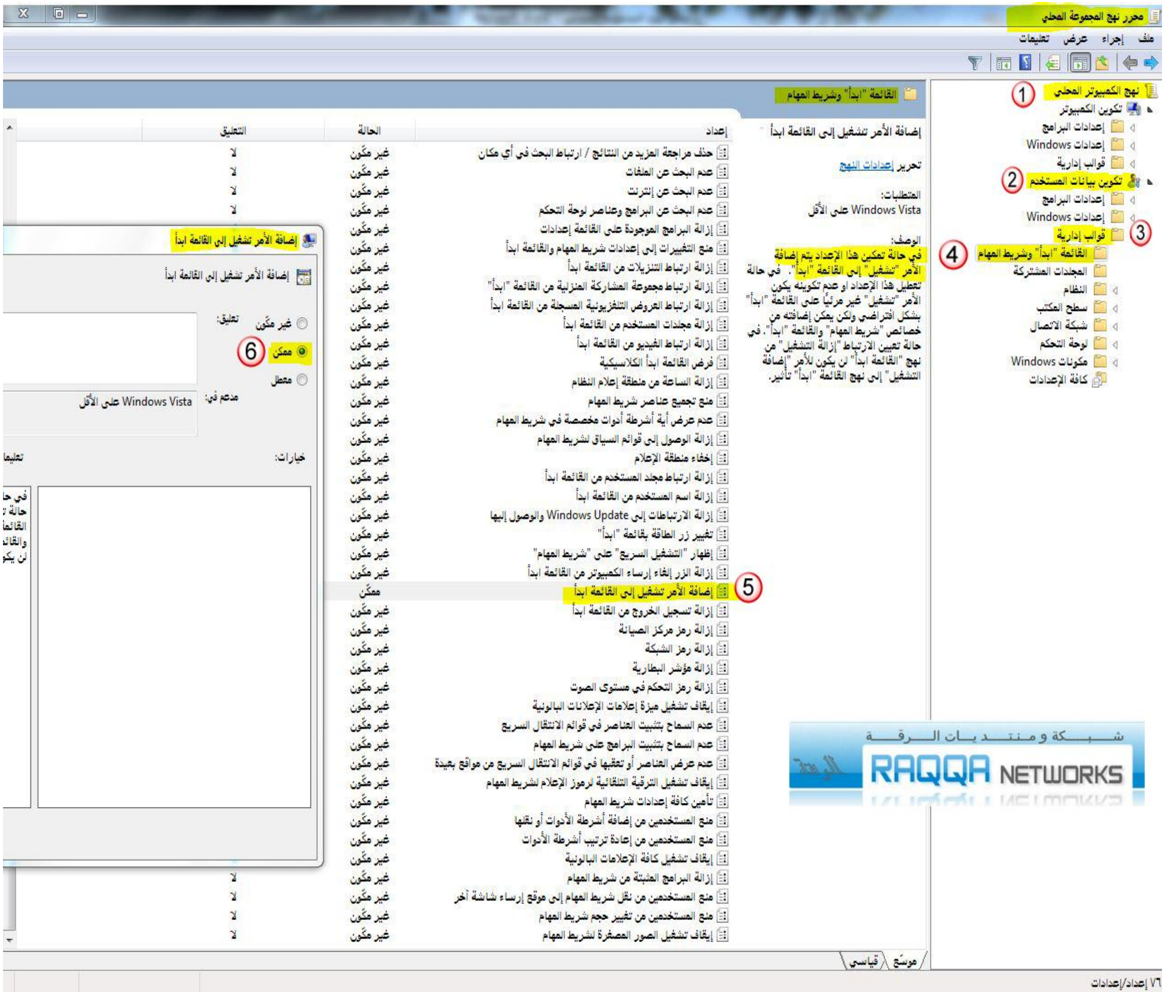
محرر نهج المجموعة المحلي + تكوين بيانات المستخدم + قوالب إدارية + القائمة ابدا وشريط المهام + أضافة الامر تشغيل الى القائمة أبدا

ننقر عليها ونختار ممكن

ثم

موافق

كما في الصورة :



صورة توضح طريق ة أضافة الامر تشغيل الى القائمة ابدا

****
****

الى هنا نصل الى نهاية الدرس

خاتمة :

من خلال محرر نهج المجموعة ستكتشف الكثير من الاعدادات الى التي تقوم بإيقافها الفيروسات

كما تستطيع تخصيص الكمبيوتر كما تشاء

كما نحاول تسهيل استعادة الإعدادات بشكل اسهل للمستخدم

عن طريق الاسطوانات التي تقوم بأوامر جاهزة تسهل استعادة الاعدادات

وهي تكون معاكسة تماما للفيروسات أي هندسة عكسية ولكن بشكل مبسط -_-

ولكن الوقت للأسف ضيق

وننتظر اكتشافاتكم ومناقشاتكم

للمشاركة نرجو منكم

زيارة المنتدى :

شبكة ومنتديات الرقة

http://www.araqqa.syriaforums.net

ووضع مناقشاتكم في قسم صيانة الكمبيوتر

ولأي استفسار راسلنا على البريد التالي :

raqqanetworks@gmail.com